情報セキュリティ自己診断チェックリスト

【はじめに】
　この自己診断チェックリストは、自分の情報セキュリティ対策についての知識の正確性・理解度を確認するものです。

　本チェックリストは、インターネットに接続できるパソコンやスマートフォンなどの機器を利用するシーンごとに、理解しておくべき知識、対策、注意事項などをクイズ形式でまとめています。本リストの全問をチェックすることで、自分が何を理解できていて、何を理解できていないのか、理解度を把握することができます。

　本リストを自分自身の情報セキュリティの向上にお役立て下さい。

内閣官房情報セキュリティセンター

0. 自己診断チェックリストについて

この自己診断チェックリストは、全22問の3択クイズです。
解答は、下にある解答欄に記入しましょう。縦には選択肢、横にはクイズ番号が並んでいます。各問の選択肢の文字に○を付けていくと、全部解き終わったときには、2つのメッセージが浮かび上がってきます。
早速問題にチャレンジして、メッセージを解読しましょう！！

【解答欄】

メッセージ1

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
A1	あ	た	よ	せ	な	み	ゆ	え	て	か	ご
A2	き	も	し	い	な	ゆ	き	り	い	い	う
A3	ら	ん	み	ん	せ	き	く	か	と	じ	ー

守って ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ！！

メッセージ2

	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22
A1	う	の	よ	は	い	ろ	た	る	あ	て	と
A2	た	り	し	い	ず	ひ	か	み	か	つ	も
A3	え	お	こ	じ	み	ん	し	ー	ね	や	み

使って ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ！！

1.　利用環境の設定

Q1/22　**新しく購入したパソコンやスマートフォンの利用環境設定時に、情報セキュリティ対策として行うべき対応のうち、最も適切な選択肢はどれでしょうか？**

A1　ウイルス対策ソフトを導入する他、起動画面にもパスワード設定を行う

A2　ウイルス対策ソフトは導入せず、起動画面にパスワードを設定する

A3　信頼できる製造メーカーの製品を購入しているため、特に対策は必要ない

2.　起動時のセキュリティ対策

パスワードを他人から推測されにくくする工夫として最も適切な選択肢はどれでしょうか？

A1　自分と特定の友人しか知り得ない合言葉をパスワードにする

A2　個人の主観がパスワードに反映されないように、複数の友人と知恵を出し合って、複雑なパスワードを作る

A3　文字だけでなく数字や記号を織り交ぜてパスワードを作る

3. セキュリティの更新

Q3/22 **パソコンやスマートフォンに導入されているOS(オーエス)※に情報セキュリティ上の欠陥が見つかりました。その情報セキュリティ対策として行うべき行動のうち、最も適切な選択肢はどれでしょうか？**

A1 ウイルス対策ソフトの更新を止める

A2 OSの修正プログラム(セキュリティパッチ)を適用する

A3 情報セキュリティ上の欠陥を放置していても、インターネットの利用には問題ない

※OS：オペレーティングシステムの略称で、パソコン全体を管理するためのソフトウェアです。具体的には、キーボードからの入力やディスプレイ、プリンタへの出力といった入出力機能などの管理を行っています。

Q4/22 **パソコンやスマートフォンのOSやソフトウェアに発見された情報セキュリティ上の欠陥を修正せずに放置した場合に考えられる状況は、どの選択肢でしょうか？**

A1 ウイルス対策ソフトを導入していれば、情報セキュリティ上の欠陥を修正しなくてもウイルスに感染することはない

A2 OSやソフトウェアに見られる情報セキュリティ上の欠陥は、対策を打たなくても時間の経過とともに自然と修復される

A3 ウイルス感染の危険性が増大する

4. 個人情報の取り扱い

Q5/22 **自分や家族・友人の個人情報※が、インターネット上に漏えいしたときに考えられる状況として間違っている選択肢はどれでしょうか？**

A1 自分の不注意で、家族や友人のプライバシーが侵害される可能性が発生する

A2 自分のプライバシーが侵害される可能性が発生する

A3 誰も全く被害を受けることはない

※個人情報：氏名、誕生日、住所、メールアドレス、電話番号、血液型、国籍、学歴など

Q6/22 **自分や家族・友人の個人情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 多くの危険を伴うファイル共有ソフト※は利用しない

A2 安易に、プライバシーに関わる個人情報はインターネット上に公開しない

A3 個人情報は、できるだけたくさんのUSBメモリやCD-Rなどに複製(バックアップ)する

※ファイル共有ソフト：不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェア。Winny,share,Cabosなどがある

5. 金融・財産情報の取り扱い

Q7/22 **金融・財産情報※が、インターネット上に漏えいした場合に考えられる状況として間違っている選択肢はどれでしょうか？**

A1 取引銀行のネットバンキングのログインパスワードが漏えいしても、銀行のキャッシュカードを紛失していなければ、不正に取引されることはない

A2 ネットバンキング用のログインパスワードが勝手に変更される

A3 自分の口座から知らぬ間に、他人に振込がされている

※金融・財産情報：口座番号・暗証番号、ネットバンキング用のログインパスワード、クレジットカード番号など

Q8/22 **金融・財産情報が、他人から盗み取られないように、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 ネットバンキングを利用した後は、入力した履歴を削除するよう心がけている

A2 ネットバンキング用のログインパスワードは、忘れると困るので、生年月日や、同じ数字を連続したものを使い続けることにしている

A3 金融機関を名乗り、口座番号やクレジットカードの有効期限、暗証番号の入力を促すメールが届いたとき、安易にそれらの情報を入力しないよう注意している

6.　思い出情報の取り扱い

Q9/22

パソコンやスマートフォンに保存されている思い出情報※が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

A1　ファイル共有ソフトを用い、不特定多数のコンピュータ間で様々なファイルを共有する

A2　セキュリティ対策ソフトを導入する

A3　漏えいして困るファイルにはパスワードをかけておく

※思い出情報：思い出に残る大切な写真や動画（家族や友人と一緒に写った写真・動画、など）

Q10/22

家族や友人と写った写真や動画をインターネット上に公開するときの行動として、間違っている選択肢はどれでしょうか？

A1　インターネット上に公開する写真などに写っている家族や友人から、その写真や動画を公開することの許可を得る

A2　きれいに撮れた写真なので、インターネット上にすぐに公開する

A3　ブログなどの日記に掲載する写真は、公開しても困らないようなものを選択して掲載する

7.　紛失したら困る重要情報の取り扱い

Q11/22

パソコンなどが故障した場合に、そこに保存している重要な情報（思い出情報など）を失わないように、日頃から注意すべき行動のうち、もっとも適切な選択肢はどれでしょうか？

A1　同じパソコンの別のフォルダにもう一つ複製（バックアップ）している

A2　故障に対するメーカーの有償修理サポートを切らさないよう注意している

A3　日頃からパソコンなどの機器が故障することに備えて、失いたくない重要な情報はUSBメモリ・外付けハードディスク・DVD-Rなどに複製（バックアップ）しておく

8. デジタルコンテンツの閲覧、入手

Q12/22 **ホームページ(ウェブ)を閲覧する時に、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

A1 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、消費生活センターや警察などに相談する

A2 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、画面に表示されている問合せ先に電話や電子メールで連絡し、入会を取り消して欲しい旨を伝える

A3 閲覧しようとするURLは、信頼できるホームページかどうか、「ホームページの信頼性評価」などの機能がついているウイルス対策ソフトを使って判断するようにしている

Q13/22 **デジタルコンテンツ※の入手(ダウンロード)に際して、注意することとして間違っている選択肢はどれでしょうか？**

A1 気になるファイルは全てとりあえずダウンロードして、後でファイルに保存されている情報を確認するようにする

A2 ファイルの提供元の名前や事業内容を確認してからダウンロードを行う

A3 ウイルス対策ソフトのパターンファイルを最新の状態に保っていることを確認したうえで、ファイルにウイルスチェックをかける

※デジタルコンテンツ：音楽、音声、映像、ゲームソフトなど

9. 電子メール利用時の注意事項

Q14/22 **電子メールの受信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？**

A1 知らないアドレスから届く電子メールに添付されているファイルは、安易に開かないように注意する

A2 電子メールの送信元のアドレスに覚えのないときには、返信して相手の名前や自分との関係を聞く

A3 覚えのないアドレスから届く電子メールは、友人や知人からのアドレス変更通知以外に、悪意のあるメールが含まれているかもしれないと考える

Q15/22 **電子メールの送信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？**

A1 携帯電話のアドレス変更通知を電子メールで一括送信するときには、それらのアドレスが送信先間に公開されないようにBcc(ビーシーシー)で送信する

A2 他人に電子メールを転送するような指示のあるメールを受信したら、なるべく早く多くの友人に電子メールを転送する

A3 誤送信の危険を減らすため、送信アドレスの入力後に再度、正しく入力されているか確認することにしている

10. ネットワークを介したゲームや情報家電の利用

Q16/22 **インターネットに接続してゲーム機器を利用するときに、情報セキュリティに関して意識しておくべき状況として間違っている選択肢はどれでしょうか？**

A1 パソコンやスマートフォンとは異なり、ゲーム機器はインターネットに接続して利用してもウイルスに感染することはない

A2 パソコンやスマートフォンと同じようにゲーム機器もウイルスに感染することがある

A3 パソコンやスマートフォンと同じようにゲーム機器もインターネットに繋がっているので、個人情報の取扱には注意が必要である

Q17/22 **インターネットに接続してゲーム機器や、デジタルテレビなどの情報家電を利用するときに、情報セキュリティ対策として意識しておくべき対応のうち、間違っている選択肢はどれでしょうか？**

A1 製造元から公開される修正プログラム(セキュリティパッチ)が公開された場合は、自動更新あるいはすぐに修正プログラムを適用する

A2 パソコンからインターネットを利用する時と同様に、パスワードは自分だけの秘密にする

A3 機器の取扱説明書に記載された設定を行ったので、それ以上特に利用時に意識しておくことはない

11. SNSやブログ利用時の注意事項

Q18/22 **SNS(エスネヌエス)※やブログの利用に関して、情報セキュリティの観点から間違っている選択肢はどれでしょうか？**

A1 SNSやブログで知り合った人との交流を広げるためにも、自分のプライバシー情報は積極的に公開して、相手から信頼を受けるようにしている

A2 友人を名乗る不審なメッセージが届いたときは、本人から直接得ている連絡先に事実確認を行うよう配慮している

A3 ブログなどの日記に掲載する写真は、公開しても誰も困らない写真を選択して掲載する

※SNS：ソーシャルネットワーキングサービスのアルファベットの頭文字をとったもので、個人の日記やフォトアルバムを特定の人に公開できたり、自分とSNS参加者が気軽に意見交換できるコミュニティを開設できたりなど、様々な機能を持った自分専用のウェブサイトです。

Q19/22 **スマートフォンを通じてSNSやブログに情報を公開することに関して間違っている選択肢はどれでしょうか？**

A1 スマートフォンで撮影した写真には、位置情報が記録されている場合もあるので、居場所の情報が知られたくない場合は、位置情報の設定を加工して知られないよう取り扱うことにしている

A2 SNSやブログのプロフィールで公開する情報は、誰に見られてもいいように取捨選択している

A3 街中でスマートフォンで撮影した写真に他人が写っている場合、自分とは関係のない人なので、特に配慮することなく公開しても問題はない

１２．　自宅外利用時

Q20/22 **紛失したら困る重要な情報が保存されたパソコンやスマートフォン、USBメモリ※などを持って外出するとき、情報セキュリティ対策上、注意すべきこととして間違っている選択肢はどれでしょうか？**

A1 機器の紛失や盗難を防ぐために、貴重品を扱うのと同様に、常に所在を意識した行動をする

A2 USBメモリの中のファイルにパスワードを設定しておく

A3 重要な情報を持っていることを周囲に気づかれないよう、持っていることを忘れて、平常通りの行動をする

※USBメモリ：持ち出し持ち運び可能な記憶装置です。

Q21/22 **外出先で無線LANに接続してインターネットを利用する場合のセキュリティに関する注意として間違っている選択肢はどれでしょうか？**

A1 パソコンのファイアウォール機能を有効にしておく

A2 電波を利用した通信形態をとる無線LANは盗聴される心配はない

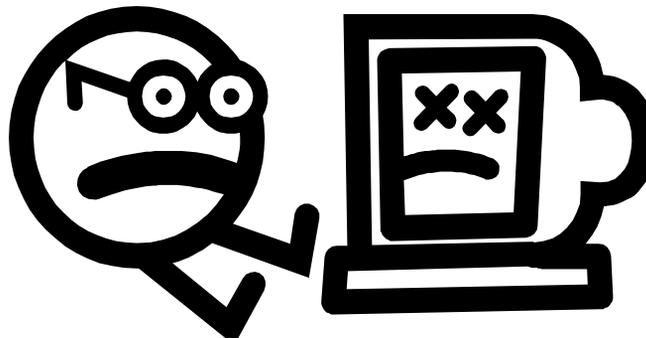
A3 漏えいして困るような情報のやりとりや、金融取引を行わないようにしている

１３．　トラブル発生時の対応

Q22/22 **インターネット利用時にコンピュータのセキュリティに何か異常を感じたとき(例えば、架空請求のメールが届いたり、開いているページを閉じることができないなど)の対応として間違っている選択肢はどれでしょうか？**

A1 数か月様子を見て、それでも異常を感じるようだったら、誰かに相談する

A2 有線回線を利用している場合は、すぐに回線を抜く

A3 困ったときは1人で悩まず、すぐに誰かに相談する

自己診断チェックリスト　黄版

解答・解説

1. 利用環境の設定

Q1/22　新しく購入したパソコンやスマートフォンの利用環境設定時に、情報セキュリティ対策として行うべき対応のうち、最も適切な選択肢はどれでしょうか？

【解答】
A1．ウイルス対策ソフトを導入する他、起動画面にもパスワード設定を行う

【解説】
　購入したばかりのパソコンやスマートフォンは、すぐにインターネットが利用できるようにアプリケーションの設定に取り掛かりたい気持ちに駆られます。
　しかし、インターネットの利便性を享受するためには、安心安全なセキュリティ環境の確保が不可欠です。インターネット上には、パソコンやスマートフォンに悪さ※をするコンピュータウイルスなどが存在します。利用する前には、ウイルス対策ソフトを導入したり、自分以外の人に勝手に機器を利用されないよう起動画面にパスワードを設定しましょう。
よってA1が適切です。

　A2は、利用環境として自分以外の人がパソコンを使用することを防ぐだけであり、情報セキュリティ対策であるウイルス対策ソフトを導入していないので、不適切です。
　A3は、信頼できるメーカーの製品だとしても、コンピュータウイルスは技術の隙間を突いたり、進化したりする特徴があります。このため、どのメーカーの製品だとしても、セキュリティ対策は必要です。

※悪さとは、パソコンなどの機器を壊したり、機器の中の個人情報や金融・財産情報を盗み取ったり、改ざんしたり、インターネット上に勝手に公開したりするものです。その結果利用者は精神的・金銭的苦痛を受けてしまいます。

2. 起動時のセキュリティ対策

パスワードを他人から推測されにくくする工夫として最も適切な選択肢はどれでしょうか？

【解答】
A3．文字だけでなく数字や記号を織り交ぜてパスワードを作る

【解説】
　パスワードを起動画面に設定していないと、自分のパソコンやスマートフォン、ゲーム機器を自分以外の人に使われてしまい、中の情報を見られたり、消されたりする危険があります。そこで、他人に使われないために、起動画面にパスワードを設定することが重要です。

　ただし、パスワードを設定しても、そのパスワードを自分以外の人がすぐに分かってしまっては意味がありません。より強いパスワードを作るためには以下のような注意が必要です。
・数字や記号、大文字、小文字を組み合わせる
・文字数を増やす（長ければ長いほどパスワードは強くなります
・氏名や住所、電話番号、車のナンバープレートのような推測しやすいパスワードは避ける

　さらに、パスワードは自分だけで管理することが大切です。選択肢A1やA2は、友人や知人にパスワードを知られていることになるので不適切です。
　同じ理由で、パスワードを忘れないようメモに残す場合でも、人目に触れる場所に貼ったりするのではなく、貴重品の保管場所と同じ場所に保管するなど、自分だけの秘密として管理しましょう。

3. セキュリティの更新

パソコンやスマートフォンに導入されているOS(オーエス)※に情報セキュリティ上の欠陥が見つかりました。その情報セキュリティ対策として行うべき行動のうち、最も適切な選択肢はどれでしょうか？

【解答】
A2. OSの修正プログラム(セキュリティパッチ)を適用する

【解説】
　コンピュータに悪さをするコンピュータウイルスやスパイウェア※１、ボット※２などの不正プログラムの中には、パソコンやスマートフォンに存在する情報セキュリティ上の欠陥（セキュリティホール）を狙ってくるものもあります。これらの機器にセキュリティホールがあると、インターネットに接続しただけでコンピュータウイルスに感染してしまうこともあります。
　製造元は、このようなセキュリティホールを発見しては、セキュリティパッチと呼ばれる修正プログラムを公開しているので、セキュリティホールを修正するために、常に最新のものを適用（アップデート）しましょう。よってＡ２が適切です。

Ａ１、Ａ３は、情報セキュリティ上の欠陥に対応していないため、ウイルスに感染しやすくなり、インターネットの利用に支障を来たす可能性があります。したがって、A1、A3ともに適切ではありません。

※１スパイウェア：スパイウェアは、情報を収集する不正プログラムであり、コンピュータに保存されている情報を収集し、悪意ある第三者に送信することを目的としています。

※２ボット：ボットとは、コンピュータを外部から操る不正プログラムです。感染すると、他のコンピュータに対して不正プログラムをばらまくなど、加害者の手先として操られてしまいます。ボットに感染したコンピュータは、被害者であると同時に、加害者になってしまうのが特徴です。

パソコンやスマートフォンのOSやソフトウェアに発見された情報セキュリティ上の欠陥を修正せずに放置した場合に考えられる状況は、どの選択肢でしょうか？

【解答】
A3. ウイルス感染の危険性が増大する

【解説】
　パソコンやスマートフォンにセキュリティホールがあると、インターネットに接続しただけでコンピュータウイルスに感染してしまうこともあります。ＯＳやソフトウェアのアップデートを行ってセキュリティホールを修正しないと（Q3解説参照）、セキュリティホールを狙う新たなウイルス感染などに繋がります。よってA３は考えられる状況です。

　Ａ１は、たとえウイルス対策ソフトを導入していたとしても、セキュリティホールがあると、ウイルスに感染してしまうこともあるので間違いです。Ａ２は、OSやソフトウェアのアップデートなどの対策を打たなくとも、セキュリティ上の欠陥が自然に修復されることはないため間違いです。

4.　個人情報の取り扱い

Q5/22　自分や家族・友人の個人情報が、インターネット上に漏えいしたときに考えられる状況として間違っている選択肢はどれでしょうか？

【解答】
A3. 誰も全く被害を受けることはない

【解説】
　電子データはその性質上、簡単にデータを複製して流通させることができるため、個人情報がひとたび漏えいすると、完全に回収することが困難です。情報が漏えいすると自分のプライバシーがインターネット上の複数のサイトに転載されたり、情報に家族や友人の個人情報が含まれている場合は、自分だけでなく家族や友人にも影響が及んだりする場合があります。よってA1、A2は正しい状況です。
　このため、「誰も全く被害を受けることはない」というA3が間違っている状況を示す選択肢です。
なお、個人情報には、以下のような項目が該当します。

- 氏名
- 生年月日
- 性別
- 血液型
- 身長
- 体重
- 身体特性
- 個人の写真
- 生体認証情報
- 人種
- 国籍
- 住所
- メールアドレス
- 電話番号
- パスポート情報
- 学歴系情報
- 勤務履歴情報
- 健康保険証情報
- 年金証書情報
- 免許番号
- 介護保険証情報
- 健康診断結果
- 趣味・嗜好
- その他プライバシー情報
（犯罪歴・政治思想など）
- 家族・友人・知人の個人情報

など

個人情報は、自分自身の情報だけではなく、家族や友人などの情報も守るように意識しましょう。

Q6/22　自分や家族・友人の個人情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A3. 個人情報は、できるだけたくさんのUSBメモリやCD-Rなどに複製(バックアップ)する

【解説】
　A1は、ファイル共有ソフトの利用についての選択肢です。ファイル共有ソフトは、不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェアなので、利用者のミスや設定の誤りによって、公開したくないファイルを公開してしまうなど、利用には危険が伴います。Ａ１は正しい行動です。

　プライバシーに関わる情報は公開前に公開する範囲（誰にどんな情報を公開するか）を判断しましょう。公開範囲を制限しないと、見知らぬ人にも自分のプライバシー情報を公開することになり、トラブルの原因になります。よってA2は正しい行動です。
　Ａ３は、漏えいしないための対策ではありません。よってA3は間違っている行動です。

5. 金融・財産情報の取り扱い

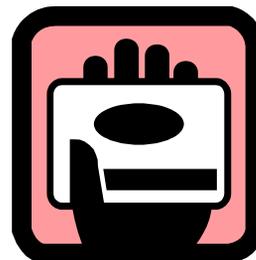
金融・財産情報が、インターネット上に漏えいした場合に考えられる状況として間違っている選択肢はどれでしょうか？

【解答】

A1. 取引銀行のネットバンキングのログインパスワードが漏えいしても、銀行のキャッシュカードを紛失していなければ、不正に取引されることはない

【解説】

金融・財産情報には以下のようなものがあります。

- 所得情報（年収・借入金・残高情報など）
- 口座番号・暗証番号
- クレジットカード番号
- 印鑑登録証明書
- 金融機関のログインアカウント
- 所有不動産情報（所在地・資産取得価額、借入情報など）
- その他、不動産情報
  （有価証券・社債・国債など）

上記のような情報が悪意のある人に知られてしまうと、自分の知らないうちにネットバンキングで利用されるなど、自分の金融財産を不正に利用される状況が考えられます。
そのような被害を防ぐために、クレジットカードや銀行口座の利用明細を確認し、身に覚えの無い取引があった場合は金融機関に連絡して利用を中止するなどの対応が必要です。
取引銀行のネットバンキング用のログインパスワードが漏えいした場合は、銀行のキャッシュカードを紛失していなくても不正に取引を行われる可能性があるので、Ａ１は間違いです。また、ログインパスワードが漏えいすると、第三者がログインパスワードを勝手に変更したり、他人の口座へとお金を振り込んだりすることも可能になります。よって、A2、A3は考えられる状況です。

【参考】

悪意のある人がこれらの情報を手に入れるのに使う代表的な手口として、フィッシングやソーシャルエンジニアリングがあります。

フィッシング：
巧妙な文面のメールなどを用いて、実在する金融機関などを装い、個人情報や金融・財産情報の入力画面に誘導して、暗証番号やクレジットカード番号などを盗み取る不正行為

ソーシャルエンジニアリング：
ネットワークシステムへの不正侵入を行うために、コンピュータ技術などを利用するのではなく、人の心理面に付け込んだ手段（話術や盗み聞き、盗み見などの「社会的」な手段）によって、パスワードなどのセキュリティ上重要な情報を入手すること

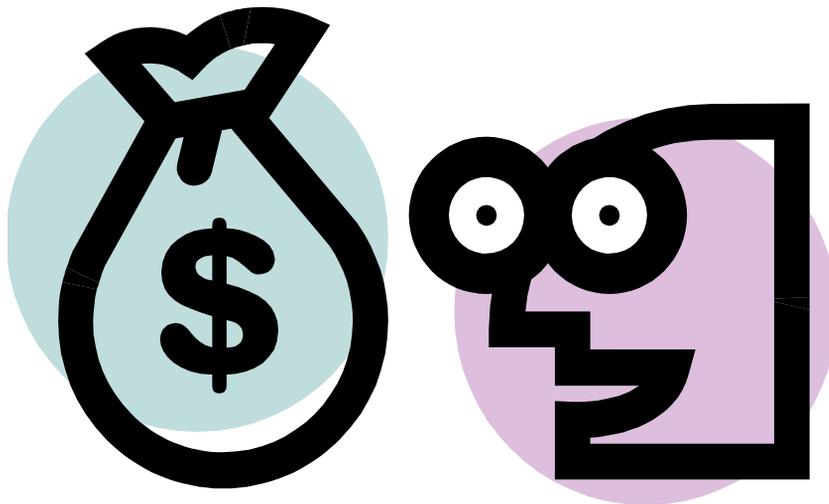
フィッシングは、ユーザを騙すことによって成り立つ不正行為であるため、怪しいメール、リンク先などを疑ってかかるなどの用心深い意識行動が対策として重要です。正規のサイトと偽造されたサイトを区別するのは困難なため、まずは、心当たりのないメールの誘導に対して暗証番号やクレジット番号を安易に入力しないよう、注意を払うことが大切です。
ソーシャルエンジニアリングは、ゴミの中から目的の情報を収集する方法、パソコン画面の覗き見や電話の盗み聞きなどによって情報を収集する方法、他人になりすまして情報を聞き出す方法などがあります。ソーシャルエンジニアリングへの対策としては、機密情報はシュレッダーにかけたり、パソコンやスマートフォンの画面にプライバシーフィルターを貼ったり、少しでも不審に感じた電話には応じないなどの方法があります。

Q8/22 金融・財産情報が、他人から盗み取られないように、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A2. ネットバンキング用のログインパスワードは、忘れると困るので、生年月日や同じ数字を連続したものを使い続けることにしている

【解説】
　パスワードは他人に推測されにくいものとし、定期的に変更するなど、他人に知られないよう管理することが必要です。Ａ２のように、他人から推測されやすいパスワードを変更せずに使い続けると、他人に知られる危険性が高まります。よってA2は間違った選択肢です。

　パスワードは、ネットバンキングなどを利用した後は、パソコン上に記録が残っている場合もあるので、入力した履歴を削除するよう、心がけることが大切です。よってＡ１は正しい行動です。
　また、Ａ3のようなメールもあるので、大切な情報をだまし取られないよう注意した行動をとりましょう。

【参考】
　最近、インターネット喫茶などの共用利用できる機器の中には、「キーロガー」と呼ばれる悪質なソフトウエアに感染しているものもあり、機器に入力したキー操作を盗み取られることがあります。実際にインターネット喫茶からのインターネットショッピングでは、入力したクレジットカード番号や暗証番号が盗み取られた事例もあるので、共同利用できる機器での金融・財産情報の取り扱いには注意が必要です。

6.　思い出情報の取り扱い

Q9/22　**パソコンやスマートフォンに保存されている思い出情報が、インターネット上に漏えいしないために、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？**

【解答】
A1. ファイル共有ソフトを用い、不特定多数のコンピュータ間で様々なファイルを共有する

【解説】
　思い出情報には、家族や友人との旅行写真や動画、日記、また思い出に残った景色などの写真や動画などが含まれます。
　家族や友人と一緒に写った写真や動画は、自分だけではなく、一緒に写った家族や友人にとっても大切な情報です。そのため、それらの写真が漏えいした場合、自分や家族、友人のプライバシーが侵害されるおそれがあります。このような被害を予防するために、セキュリティソフトを導入したり、漏えいして困るファイルにパスワードを設定することは、有効な対策です。よって、A2、A3は適切な行動です。

　ファイル共有ソフトを用いて不特定多数とファイルの共有や交換を行うと、利用者のミスや設定の誤り、ウイルス感染などによる漏えいの危険が高まります。よってＡ１は間違いです。

Q10/22　**家族や友人と写った写真や動画をインターネット上に公開するときの行動として、間違っている選択肢はどれでしょうか？**

【解答】
A2. きれいに撮れた写真なので、インターネット上にすぐに公開する

【解説】
　自分や家族、友人のプライバシーに係わる情報を公開する時には、本人に許可を取ることがマナーです。人によっては公開を快く思わない人もいるので、許可が得られないときは、インターネットでは公開しないことがトラブル防止に有効です。よってＡ１は正しい行動です。
　また、ひとたび公開するとそれらのデータが様々なサイトに転載され回収が難しくなることもあるので、公開しても困らないものを選択することが重要です。よってＡ３は正しい行動です。
　本人の許可を取ること無く、すぐに公開することは、マナー違反であるばかりでなく、本人とのトラブルの原因になりかねません。よってＡ２は間違った行動です。

7. 紛失したら困る重要情報の取り扱い

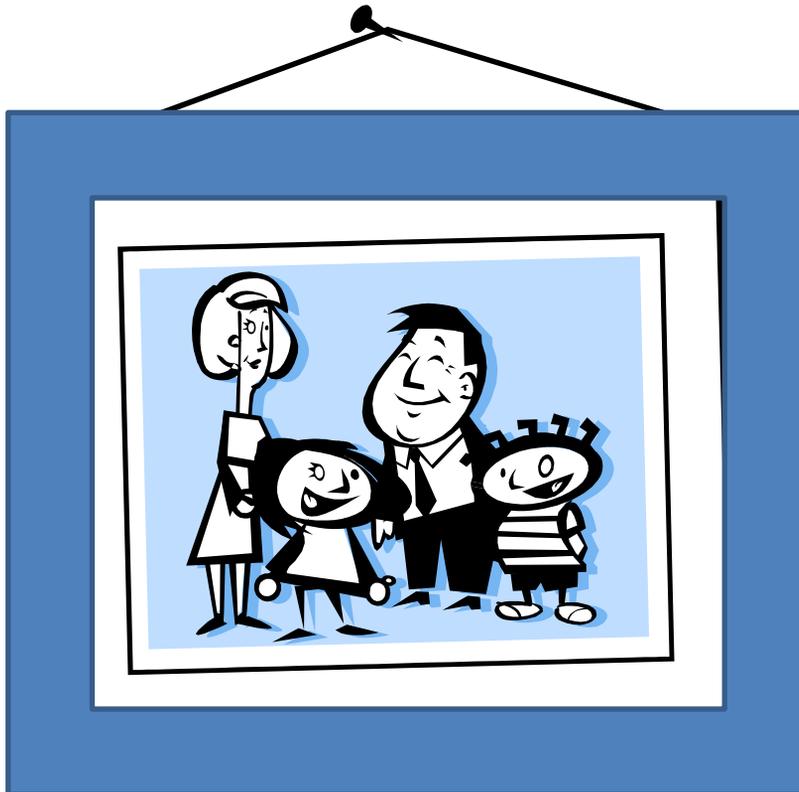
Q11/22 **パソコンなどが故障した場合に、そこに保存している重要な情報（思い出情報など）を失わないように、日頃から注意すべき行動のうち、もっとも適切な選択肢はどれでしょうか？**

【解答】

A3. 日頃から、パソコンなどの機器が故障することに備えて、失いたくない重要な情報はUSBメモリ・外付けハードディスク・DVD-Rなどに複製（バックアップ）しておく

【解説】

パソコン上に保存している情報は、パソコンが故障した場合、失われることが想定されます。
そこで、失いたくない重要な情報は、予め複製（バックアップ）を取得しておくことが日頃の備えとして有効です。よってＡ３が適切な行動です

Ａ１は、保存場所が適切ではありません。同じパソコン内に複製すると、パソコンが故障した場合に取り出せなくなります。
Ａ２は、故障自体の修繕には、メーカーサポートは有効ですが、有償サポートの場合でも、多くの場合、パソコンの中のデータまでは保証してくれません。よってＡ２は適切ではありません。

8． デジタルコンテンツの閲覧・入手

Q12/22 ホームページ（ウェブ）を閲覧する時に、日頃から注意すべき行動として間違っている選択肢はどれでしょうか？

【解答】
A2. 画像やリンクをクリックしたときに、意図しない入会完了画面や料金請求画面が表示されたときには、画面に表示されている問合せ先に電話や電子メールで連絡し、入会を取り消して欲しい旨を伝える

【解説】
Ａ１は適切な行動です。トラブルが発生した場合は、一人で悩まずに、身近な人や各種相談窓口に相談しましょう。
Ａ３のように、ウイルス対策ソフトのなかには、閲覧しようとするＵＲＬが信頼できるかどうかを表示する機能を持つものもあります。このような機能を活用して、ウイルス感染を避けながらホームページ(ウェブ)閲覧を楽しみましょう。よってA3は適切な行動です。

URLをクリックしただけで、意図しない入会完了画面や料金請求画面が表示され、それを信用してお金を振り込んでしまう被害は“ワンクリック詐欺”と呼ばれています。これらの画面が表示されたら、無視することが適切な対策の1つです。架空の請求画面に表示されている問合せ先に連絡してしまうと、連絡に使った電話番号やメールアドレスにも請求がくるようになり、事態が悪化することもあるので、Ａ２の対応は適切ではありません。

Q13/22 デジタルコンテンツの入手（ダウンロード）に際して、注意することとして間違っている選択肢はどれでしょうか？

【解答】
A1. 気になるファイルは全てとりあえずダウンロードして、後でファイルに保存されている情報を確認するようにする

【解説】
インターネットには悪意のある人も存在します。悪意のある人が提供するファイルにはウイルスが含まれている危険があります。そのため、ファイルをダウンロードするときに提供者の名前や事業内容をインターネットで確認するなど、信頼できる相手かどうか判断することが大切です。よってA2は適切な行動です。

また、インターネットでダウンロードできるファイルには新種のウイルスを含むものもあります。セキュリティソフトの有効期限が切れたまま、安易にファイルをダウンロードすると、新種のウイルスに感染する危険が高まります。Ａ３に示すようにウイルス対策ソフトは最新のものに更新し、新種のウイルス感染への対策を行いましょう。

A1のように、気になるからといって安易にダウンロードするのは情報セキュリティ上望ましくありません。ウイルスを含んだファイルがパソコンに侵入しないように慎重な行動を心がけましょう。よって、A1は適切な対応ではありません。

９．　電子メール利用時の注意事項

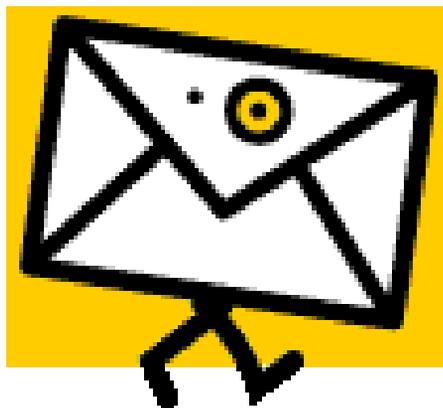
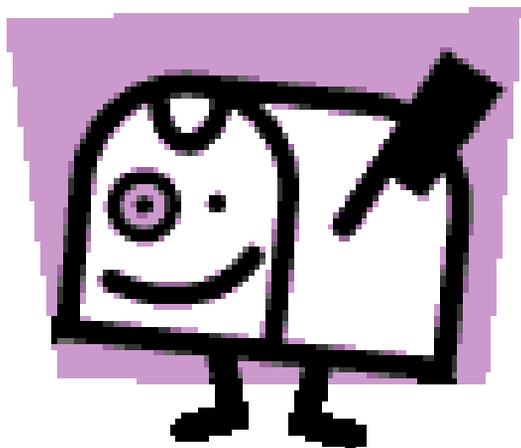
Q14/22 電子メールの受信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？

【解答】
A2. 電子メールの送信元のアドレスに覚えのないときには、返信して相手の名前や自分との関係を聞く

【解説】
　知らないアドレスから電子メールが届いたときは注意を払う必要があります。知らないアドレスからメールが届く場合の例として以下のような場合が考えられます。よってA3は適切です。

・家族や友人からのアドレス変更通知
・家族や友人に紹介された知人から届く初めてのメール
・コンビニやレンタルビデオ店のサービス紹介メール
・架空請求メールやウイルスを媒介するメール　など

　添付ファイルにはウイルスが含まれている可能性もありますので、Ａ1のように安易に添付ファイルを開かないようにしましょう。Ａ1は適切です。

　返信して名前や自分との関係を聞くのは危険です。返信することでよりたくさんの迷惑メールが届くようになったりするので、安易に返信はしないようにしましょう。よってＡ2は不適切です。

Q15/22 電子メールの送信に関して、注意すべき観点として間違っている選択肢はどれでしょうか？

【解答】

A2. 他人に電子メール転送するような指示のあるメールを受信したら、なるべく早く多くの友人に電子メールを転送する

【解説】

Ａ２のような電子メールをチェーンメールといいます。このメールの特徴は、電子メールを多くの人に送信させるというものです。このような電子メールが届いた場合は、転送しないでそのまま削除するようにしましょう。チェーンメールを転送してしまうと、ネズミ算式にメールが増加するため、ネットワークやメールサーバーに負荷がかかり、通信速度が遅くなるなどの影響が多くの人に及ぶ可能性があります。よって、Ａ２は間違った選択肢です。

メールを送信するときには、To(トゥー)、Cc(シーシー)、Bcc（ビーシーシー）の3つの宛先指定方法を使い分けることが重要になってきます。

・To・・・・メールの宛先となる相手のアドレスを入れます。そのメールを受信した人全員が、Toに指定されたアドレスを見ることができます。

・Cc・・・・「Toに宛てたメール」のコピーを送る相手のアドレスを入れます。Toと同様に、そのメールを受信した人全員が、Ccに指定されたアドレスを見ることができます。

・Bcc・・・・用途はCcと同じですが、Bccに指定されたアドレスは、そのメールを受信した人に見られることはありません。

携帯電話やスマートフォンのメールアドレスを変更し、その連絡をするときなど、お互いがメールアドレスを知らない複数の人に一斉にメールを送りたいときに、Bccを使用します。よってA１は適切です。

また、Ａ３のように、誤送信を防ぐためには、送信アドレスに入力した内容は、送信する前に再度正しいアドレスが入力されているか確認したうえで送信しましょう。よってA３は適切です。

１０．ネットワークを介したゲームや家電機能の利用

Q16/22 インターネットに接続してゲーム機器を利用するときに、情報セキュリティに関して意識しておくべき状況として間違っている選択肢はどれでしょうか？

【解答】
A1. パソコンやスマートフォンとは異なり、ゲーム機器はインターネットに接続して利用してもウイルスに感染することはない

【解説】
インターネットに接続してゲーム機器を利用するときは、それが単なるゲームではなく、パソコンやスマートフォンを使ってインターネットに接続している環境と類似していることを意識しておくことが重要です。ゲーム機器がウイルスに感染することも考えられます。よってＡ1は間違いであり、Ａ2は適切です。

また、ゲーム機器がインターネットに繋がっていることを意識して、「４．個人情報の取り扱い」「５．金融・財産情報の取り扱い」でとりあげたような被害を受けないよう、注意を払って行動することが必要です。よってＡ3は適切です。

【参考】
家庭用ゲーム機器は、ネットワークの接続も行えるなど、ゲーム以外の用途において多機能化が進んでいるため、近い将来、コンピュータウイルス感染や不正アクセス、金銭目的のサイバー犯罪などの標的になるといった、情報セキュリティ上の懸念が顕在化してきています。
（出典：「情報家電におけるセキュリティ対策　検討報告書」独立行政法人　情報処理推進機構）

Q17/22 インターネットに接続してゲーム機器や、デジタルテレビなどの情報家電を利用するときに、情報セキュリティ対策として意識しておくべき対応のうち、間違っている選択肢はどれでしょうか？

【解答】
A3. 機器の取扱説明書に記載された設定を行ったので、それ以上特に利用時に意識しておくことはない

【解説】
ゲーム機器やデジタルテレビなどの情報家電に搭載されているＯＳやソフトウェアにも、セキュリティホールが発見される場合があり、これらの情報家電においても、パソコンなどと同様に修正プログラム（セキュリティパッチ）がメーカーから無料で提供されています。インターネットに接続される機器は、ウイルス感染やスパイウェア、ボットなどの攻撃対象となりえるため、提供された修正プログラムはすぐに適用して、セキュリティホールの修正を行いましょう。よってＡ１は正しい対応です。
したがってＡ3のように、機器の取扱説明書に記載された設定を行っただけで、セキュリティ対策は完ぺきということにはなりません。よってＡ３は適切な対応ではありません。

また、漏えいしたら困る情報については、情報家電において扱う場合でも、パソコンからの利用時と同様の注意が必要です。よってＡ２は正しい対応です。

【参考】
あるゲーム機器では、セキュリティホールが発見され、修正プログラムが公開されました。
今後、情報家電などの多機能化に伴い、パソコンなどと同じように、修正プログラム情報の公開が増えてくることが予想されます。

１１．SNSやブログ利用時の注意事項

Q18/22 SNSやブログの利用に関して、情報セキュリティの観点から間違っている選択肢はどれでしょうか？

【解答】
A1. SNSやブログで知り合った人との交流を広げるためにも、自分のプライバシー情報は積極的に公開して、相手から信頼を受けるようにしている

【解説】
SNSやブログでは、参加者が本人であるか確認しにくいため、なりすましの可能性が疑われる場合には、本人から直接得ている連絡先等に事実確認をするとよいでしょう。よってA2は正しい選択肢です。
また、コミュニケーションを楽しむコミュニティであるからこそ、様々な人が参加しているので、日記に掲載する写真は、公開しても誰も困らないようなものを選択するなどの配慮も必要です。よってＡ３は正しい選択肢です。
コミュニケーションを楽しみたいがために、自分のプライバシーを積極的に公開することは、正しい行動とはいえません。よってＡ１は間違った選択肢です。

Q19/22 スマートフォンを通じてSNSやブログに情報を公開することに関して間違っている選択肢はどれでしょうか？

【解答】
A3. 街中でスマートフォンで撮影した写真に他人が写っている場合、自分とは関係のない人なので、特に配慮することなく公開しても問題はない

【解説】
スマートフォンで撮影した写真には、位置情報が記録されている場合があります。このことを知らずに、自分で撮影した写真データをブログなどに公開した場合、それを閲覧した人から、撮影位置を特定されることになります。自宅の写真を公開した場合には、自宅が特定されることになります。このため、居場所の情報が知られたくない場合は、写真データのプロパティに記録されている位置情報を加工するなどして、公開しても位置情報を知られないよう取り扱いましょう。よってＡ１は正しい選択肢です。
また、SNSやブログのプロフィール（氏名や顔写真などの個人を特定する情報、電話番号など）で公開する情報は、誰の目に触れるかわかりません。ストーカーなどの被害も考えられるため、適切に取捨選択したうえでの利用が求められます。よってＡ２は正しい選択肢です。
一方、Ａ３については、Ｑ１０の解説と同様に、写真に写ってしまった人のプライバシーを侵害する可能性があるので、顔を特定できないよう加工するなど、配慮が必要です。よってＡ３が間違った選択肢です。

１２．自宅外利用時

Q20/22 紛失したら困る重要な情報が保存されたパソコンやスマートフォン、USBメモリなどを持って外出するときは、情報セキュリティ対策上、注意すべきこととして間違っている選択肢はどれでしょうか？

【解答】
A3. 重要な情報を持っていることを周囲に気づかれないよう、持っていることを忘れて、平常通りの行動をする

【解説】
紛失したら困る重要な情報の入ったパソコンやスマートフォンを持って外出するときは、紛失や盗難に気をつけましょう。USBメモリなどの小さなものの紛失にも気をつけましょう。よってＡ１は正しい選択肢です。
また、気を付けていても紛失する場合が考えられます。そこで、予め紛失したときのことを想定して、パソコンやスマートフォンなどには起動時にパスワードを入力するよう設定しましょう。USBメモリの場合は、中のファイルにパスワードを設定しておきましょう。よってＡ２は正しい選択肢です。

Ａ３のように、注意力を持たない行動は紛失に繋がりかねないので、正しい選択とは言えません。情報漏えいなどのセキュリティ事故は、人の注意不足によるものが多いことからも、セキュリティに対する意識を保つことの重要性が指摘されています。よって、Ａ３は間違った選択肢です。

Q21/22 外出先で無線LANに接続してインターネットを利用する場合のセキュリティに関する注意として間違っている選択肢はどれでしょうか？

【解答】
A2. 電波を利用した通信形態をとる無線LANは盗聴される心配はない

【解説】
無線LANは、電波を利用して通信を行うため、電波の届く範囲であれば、どこからでもネットワークに接続ができる便利な仕組みです。一方で、発信された電波は第三者でも傍受することが可能であるため、盗聴される危険性があります。よってA2は間違った選択肢です。

無線LANには、盗聴を防ぐために暗号化の機能が用意されていますが、中には解読されやすい暗号化方式を採用しているアクセスポイントもあります。漏えいして困るような情報は安易に扱わないように注意することが大切です。よってＡ３は正しい選択肢です。

また、無線LANを通じて第三者から自分のパソコンを侵害されることを防ぐために、ファイアーウォール機能を有効にしておくことも適切な対策です。よってA１は正しい選択肢です。

13. トラブル発生時の対応

Q22/22 **インターネット利用時にコンピュータのセキュリティに何か異常を感じたとき(例えば、架空請求のメールが届いたり、開いているページを閉じることができないなど)の対応として間違っている選択肢はどれでしょうか？**

【解答】
A1. 数か月様子を見て、それでも異常を感じるようだったら、誰かに相談する

【解説】
インターネット利用時に、不審なファイルを実行してしまって以来パソコンの動作がおかしい、開いているページを閉じることができないなどの異常を感じたら、コンピュータがウイルスに感染している可能性があります。ウイルス感染は、自分1人のトラブルだと考えがちですが、実は周りにも迷惑をかけてしまうことがあります。例えば、他の人のパソコンに自分のパソコンが攻撃を仕掛けることもあります。
このようなトラブルが発生したときには急いで対応することが必要です。時間がたってからでは、ウイルス感染による被害が拡大します。よってA１は間違った対応です。

ウイルス感染時の行動は、まずウイルスに感染したと思われるパソコンをネットワークから切り離すことで感染が広がらないようにします。よってA２は正しい対応です。

また、ウイルス感染だけでなく、架空請求やワンクリック詐欺などのトラブルに遭ったら、1人で悩まず誰かに相談しましょう。近所のセキュリティに詳しい人や、以下の情報セキュリティ相談窓口に症状に応じて相談するとよりスムーズにトラブルを解決できるかもしれません。よってA3は正しい対応です

- 購入した製品の具体的な使い方については取扱説明書などに記載されている連絡先へご連絡ください
  - ✓各製品の開発元/販売元
  - ✓電話番号　各製品の取扱説明書などに記載されています
- コンピュータウイルスに感染してしまったと思ったらこちらにご相談ください
  - ✓IPA(情報処理推進機構)セキュリティセンター　安心相談窓口
  - ✓電話番号　03-5978-7509(平日10:00～12:00 および 13:30～17:00)
- 広告や宣伝目的の迷惑メールに困っている時はこちらへご連絡ください
  - ✓財団法人日本データ通信協会　迷惑メール相談センター
  - ✓電話番号　03-5974-0068(平日10：00～17：00)(祝祭日は除く)
- 犯罪に係る相談や情報提供を電話で受け付けています
  - ✓各都道府県警察のサイバー犯罪相談窓口
  - ✓電話番号　各都道府県警察にお問い合わせ下さい